View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Universitas Kanjuruhan Malang: Journal Unikama

EVALUASI KEAMANAN DATA PADA BANK PERKREDITAN RAKYAT XYZ MELALUI AUDIT TATA KELOLA TEKNOLOGI INFORMASI BERDASARKAN KERANGKA KERJA COBIT 4.1

Abdul Aziz[1]
[1] Teknik Informatika, Universitas Kanjuruhan Malang
[1] Abdul.aziz@unikama.ac.id

***Abstrak*—Sebuah organisasi atau institusi harus dapat memberikan jaminan terhadap kepastian keaman data. Hal ini juga yang harus dilakukan oleh BPR XYZ. Untuk menjamin keberlanjutan operasional, maka perlu dilakukan analisis terhadap tata kelola teknologi informasi yang digunakan. Tujuannya untuk memastikan apakah teknologi informasi yang ada sudah digunakan sebaik-baiknya. Jika terjadi penyalahgunaan, maka dapat menimbulkan beberapa permasalahan atau kerugian. Resiko yang harus ditanggung oleh perusahaan adalah tidak akuratnya informasi yang disebabkan oleh hilangnya data atau telah terjadi manipulasi terhadap data. Sehingga dapat menimbulkan kesalahan dalam pengambilan keputusan. Kerangka kerja COBIT 4.1 dipilih sebagai alat untuk melakukan analisis tata kelola teknologi informasi. Nilai kematangan yang didapatkan dari analisis yang telah dilakukan berdasarkan COBIT 4.1 pada domain *Aquire and Implement* (AI) dan *Delivery and Support* (DS) mendapatkan nilai 2,38 dari rentang nilai 0 sampai 5. Hal ini bisa disimpulkan bahwa tata kelola teknologi informasi pada BPR XYZ berada pada skala 2 (*Repeatable but intuitive*).**

***Kata Kunci*—Keamanan data, Audit, Tata kelola, Teknologi informasi, COBIT 4.1, Maturity Level.**

I. PENDAHULUAN

Setiap organisasi atau institusi pasti membutuhkan peran teknologi informasi dalam kegiatan operasional setiap harinya. Sistem informasi yang digunakan memiliki peran sentral pada setiap kegiatan operasional, dan pengambilan keputusan oleh manajemen juga berdasarkan data yang dihasilkan oleh sistem. Oleh sebab itu keamanan data merupakan kebutuhan yang harus dipenuhi untuk merealisasikan tujuan dari organisasi. Resiko yang harus ditanggung oleh perusahaan adalah tidak akuratnya informasi yang disebabkan oleh hilangnya data atau telah terjadi manipulasi terhadap data sehingga dapat menimbulkan kesalahan dalam pengambilan keputusan.

Hal ini berlaku pula di BPR (Bank Perkreditan Rakyat) XYZ, dimana setiap pengambilan keputusan oleh pihak manajemen berdasarkan data yang didapatkan dari sistem informasi yang digunakan. Sistem informasi yang digunakan pada BPR XYZ mencakup seluruh kegiatan utama perbankan yang terkait dengan produk Tabungan, Deposito, dan Kredit. Semua kegiatan transaksi yang dilakukan oleh nasabah akan diproses menggunakan sistem ini sehingga menghasilkan laporan keuangan perusahaan.

Dengan peran yang sangat besar tersebut, keamanan data merupakan kebutuhan yang tidak bisa ditawar lagi dan harus dipenuhi. Sehingga semua yang sudah direncanakan oleh perusahaan dapat terlaksana dengan baik tanpa ada kekhawatiran dengan validitas informasi yang dihasilkan oleh sistem. Mekanisme dan proses perawatan dan pemeliharaan sistem keamanan data/informasi secara menyeluruh belum memiliki arah yang jelas dan masih memiliki bergantung kepada kebutuhan unit kerja masing-masing [1]. Memiliki tata kelola teknologi informasi secara tepat, akurat dan relevan meningkatkan nilai-nilai ekspektasi untuk semua pemangku kepentingan [2]. Untuk itu perlu dilakukan analisis terhadap tata kelola teknologi informasi untuk meningkatan keamanan data pada BPR XYZ. Kerangka kerja COBIT 4.1 *(Control Objectives For Information and Relation Technology)*, dipilih sebagai alat untuk melakukan analisis.

Permasalahan yang dibahas di sini adalah bagaimana mengevaluasi keamanan data melalui audit tata kelola teknologi informasi untuk mengetahui tingkat kematangan berdasarkan kerangka kerja COBIT 4.1 dan memberikan rekomendasi sistem keamanan sesuai standar kerangka kerja COBIT 4.1. Tingkat kematangan tata kelola teknologi informasi pada BPR XYZ ditentukan dengan menggunakan proses AI2 dan AI3 pada domain AI (*Aquire and Implement*) dan proses DS3,DS5,DS11, dan DS12 pada domain DS (*Delivery and Support*) dan penggunaan *Maturity Level* untuk menilai tingkat kematangan. Tujuan yang ingin dicapai adalah mengetahui pengelolaan dan tingkat kematangan tata kelola teknologi informasi di BPR XYZ dan memberikan saran berdasarkan hasil pengukuran tingkat kematangan tata kelola teknologi informasi berdasarkan kerangka kerja COBIT 4.1.

II. METODE PENELITIAN

Metode penelitian yang digunakan memiliki tahapan sebagai berikut :

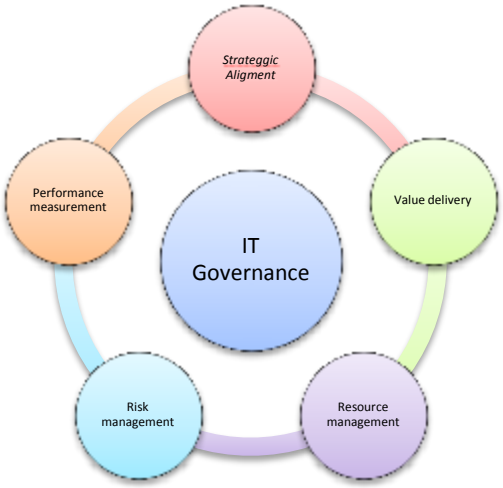
1. Identifikasi masalah
   Identifikasi masalah dilakukan untuk mendapatkan permasalahan yang terdapat pada BPR XYZ. Kegiatan ini diawali dengan menghimpun data pada obyek penelitian melalui wawancara kepada pegawai dan direksi, observasi terhadap proses kegiatan dan analisis dokumen perusahaan.
2. Kajian pustaka
   Pada tahap ini mempunyai target mendapatkan landasan teori dari kajian pustaka yang dilakukan untuk mendukung penelitian yang sedang dilakukan.
3. Pemetaan
   Menganalisa strategi bisnis perusahaan terhadap tata kelola teknologi informasi dan kemudian memetakannya ke dalam kendali proses sesuai kerangka kerja COBIT 4.1.
4. Penilaian kematangan
   Pada tahap ini dilakukan pengukuran tingkat kematangan tata kelola teknologi informasi pada perusahaan dengan menyebarkan kuesioner kepada pegawai dan direksi.
5. Hasil dan rekomendasi
   Tingkat kematangan tata kelola teknologi informasi sudah didapatkan pada tahap ini. Rekomendasi perbaikan diusulkan berdasarkan sesuai gap yang dihasilkan pada pengukuran tingkat kematangan.

Gambar 1. Metode Penelitian

Menurut [3] penanggung jawab tata kelola teknologi informasi pada perusahaan adalah dewan direksi dan manajemen tingkat atas. Strategi dan tujuan organisasi direncanakan dan disusun oleh dewan direksi dan manajemen untuk kemudian diimplementasikan dalam operasional perusahaan.

Dalam [4] disebutkan bahwa tata kelola teknologi informasi merupakan sebuah kegiatan yang melibatkan dewan, manajemen eksekutif dan manajemen teknologi informasi untuk mengendalikan rencana dan implementasi strategi teknologi informasi serta memastikan perpaduan dari bisnis dan teknologi informasi.

Teknologi informasi dapat membawa risiko, saat melakukan bisnis dalam skala global, *downtime* sistem dan network telah menjadi terlalu mahal bagi semua perusahaan untuk ditangani. Di beberapa industri, teknologi informasi merupakan sumber daya kompetitif untuk melakukan diferensiasi dan memberikan keunggulan kompetitif sedangkan diperusahaan lainnya teknologi informasi membantu dalam mempertahankan hidup perusahaan [5].



Gambar 2. Area fokus tata kelola teknologi informasi

Area fokus tata kelola teknologi informasi dibagai menjadi 5 bagian yaitu *Strategic alignment*, *Value delivery*, *Resource management*, *Risk management*, dan *Performance measurement* seperti ditampilkan pada gambar 2 dengan penjelasan sebagai berikut :

1. *Strategic Aligment*: Memastikan keterkaitan antara bisnis dengan ketentuan rencana teknologi informasi, pemeliharaan serta validasi usulan nilai teknologi informasi, dan menyelaraskan tujuan bisnis dan tujuan teknologi informasi.
2. *Value delivery*: Menjalankan proposisi nilai seluruh siklus delivery, memastikan bahwa teknologi informasi memberikan manfaat sesuai dengan tujuan bisnis yang dituangkan dalam strategi, berkonsentrasi pada biaya mengoptimalkan dan membuktikan nilai intrinsik dari teknologi informasi.
3. *Resource management*: Investasi yang optimal dalam pengelolaan sumber daya teknologi informasi: aplikasi, informasi, infrastruktur dan SDM dan pengoptimalisasian infrastruktur.
4. *Risk management*: Tentang kesadaran mengelola risiko oleh pejabat senior pada perusahan, bagaimana memahami persyaratan kepatuhan, keterbukaan tentang risiko yang signifikan terhadap perusahaan dan menanamkan tanggung jawab manajemen risiko ke dalam organisasi.
5. *Performance measurement*: Pengukuran kinerja dan track implementasi strategi, penyelesaian proyek, penggunaan sumber daya, kinerja proses dan pelayanan, misalnya, balanced scorecard yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan yang terukur.

Control Objective for Information and Related Technologi (COBIT) memberikan kebijakan yang jelas dan praktik yang baik dalam tata kelola teknologi informasi dengan membantu manajemen senior dalam memahami dan mengelola risiko yang terkait dengan tata kelola teknologi informasi dengan cara memberikan kerangka kerja tata kelola teknologi informasi dan

panduan tujuan pengendalian terinci / *detailed control objective* bagi pihak manajemen, pemilik proses bisnis, pengguna dan juga auditor.

Untuk membuat teknologi informasi berhasil dalam menyampaikan kebutuhan bisnis perusahaan, manajemen harus membuat sistem pengendalian internal atau kerangka kerja. Kerangka kerja COBIT memberikan kontribusi pengendalian kebutuhan ini dengan [6]:

- Membuat link dengan kebutuhan bisnis perusahaan
- Mengorganisasikan kegiatan teknologi informasi kedalam suatu proses yang berlaku umum
- Mengidentifikasi sumber daya teknologi informasi utama yang harus dihitung.
- Menentukan tujuan pengendalian manajemen.

Model kematangan (*maturity model*) digunakan sebagai alat untuk melakukan *benchmarking* dan *self-assessment* oleh manajemen teknologi informasi secara lebih efisien. Tingkat kematangan pemanfaatan teknologi informasi memiliki perbedaan dalam setiap level. Tingkat kematangan dalam COBIT dibedakan menjadi 6 level yaitu *non-existent*, *initial*, *repeatable*, *define*, *managed*, dan *optimised*. Dalam COBIT tiap level ini disebut dengan skala tingkat kematangan[7].

Penentuan tingkat untuk menilai tingkat kematangan akan berbeda di tiap proses teknologi informasi dengan masing-masing kriteria pemenuhannya[8]. Perhitungan nilai index kematangan untuk masing-masing obyektif hasil penelitian dengan rumus berikut ini :

$$Nilai\ Index = \sum \frac{(jumlah\ jawaban\ x\ nilai\ kematangan)}{(jumlah\ pertanyaan\ x\ jumlah\ responden)}$$

Dengan skala pembulatan indeks untuk pemetaan proses teknologi informasi ke tingkat model kematangan (Tabel 1).

Tabel 1. Skala Pembulatan Indeks

Skala	Tingkat Model Kedewasaan (Maturity)
4,51 – 5,00	5 – Sempura, IT berjalan dengan baik dan Perusahaan cepat beradaptasi terhadap perubahan (*Optimised*)
3,51 – 4,50	4 – Dilakukan Ada Prosedure, dan baku serta ada monitoring (*Managed and Measurable*)
2,51 – 3,50	3 – Dilakukan dan sudah baku (*Define*)
1,51 – 2,50	2 – Dilakukan tetapi belum baku (*Repeatable but intuitive*)
0,51 – 1,50	1 – Dilakukan tetapi tidak ada prosedur (*Initial/Ad Hoc*)
0,00 – 0,50	0 – Tidak ada proses teknologi informasi (*Non-Existent*)

Model kematangan memiliki tingkatan pengelompokkan kapabilitas pengelolaan proses teknologi informasi dari tingkat 0 (nol/*non-existent*) hingga tingkat 5 (*optimised*) dalam bentuk grafis (Gambar 3) dengan deskripsi masing-masing tingkat kedewasaan secara umum (Tabel 2).

Tabel 2. Model Kematangan

Level	Keterangan
0 *Non Existence*	Kekurangan yang menyeluruh terhadap proses apapun yang dapat dikenali. Perusahaan bahkan tidak mengetahui bahwa terdapat permasalahan-permasalahan yang harus diatasi
1 *Initial/ Ad Hoc*	Terdapat bukti bahwa perusahaan mengetahui adanya permasalahan yang harus diatasi. Bagaimanapun juga tidak terdapat proses standar, namun menggunakan pendekatan *ad hoc* yang cenderung diberlakukan secara individu atau berbasis per kasus. Secara umum pendekatan kepada pengelolaan proses tidak terorganisasi
2 *Repeatable but intuitive*	Proses dikembangkan ke dalam tahapan yang prosedur serupa diikuti oleh pihak-pihak yang berbeda untuk pekerjaan yang sama. Tidak terdapat pelatihan formal atau peng-komunikasian prosedur standar dan tanggung jawab diserahkan kepada individu masing-masing. Terdapat tingkat kepercayaan yang tinggi terhadap pengetahuan individu sehingga kemungkinan kesalahan besar dapat terjadi.
3 *Defined*	Prosedur distandarisasi dan didokumentasikan kemudian dikomunikasikan melalui pelatihan. Kemudian diamanatkan bahwa proses-proses tersebut harus diikuti. Namun penyimpangan tidak mungkin dapat terdeteksi. Prosedur sendiri tidak lengkap namun sudah memformalkan praktek yang berjalan
4 *Managed and Measurable*	Manajemen mengawasi dan mengukur kepatutan terhadap prosedur dan mengambil tindakan jika proses tidak dapat dikerjakan secara efektif. Proses berada di bawah peningkatan yang konstan dan penyediaan praktek yang baik. Otomatisasi dan perangkat digunakan dalam batasan tertentu
5 *Optimised*	Proses telah dipilih ke dalam tingkat praktek yang baik, berdasarkan hasil dari perbaikan berkelanjutan dan pemodelan kedewasaan dengan perusahaan lain. Teknologi informasi digunakan sebagai cara terintegrasi untuk mengotomatisasi alur kerja, penyediaan alat untuk peningkatan kualitas dan efektivitas serta membuat perusahaan cepat beradaptasi

III. HASIL DAN PEMBAHASAN

Berdasarkan hasil identifikasi dapat dipetakan proses bisnis teknologi informasi pada BANK XYZ sebagai berikut :

Tabel 2. Identifikasi Domain Cobit 4.1

Domain	Proses
Aquire and	AI2, AI3

Implement	
Delivery and Support	DS3, DS4, DS5, DS11, DS12, DS13

Dari setiap proses teknologi informasi terdapat *Detail Control Objectives* yang merupakan alat kontrol dari proses teknologi informasi itu sendiri. Berdasarkan penelitian yang dilakukan terdapat 27 *Detail Control Objectives* seperti tabel berikut ini :

Tabel 3. Proses Teknologi Informasi *Control Object*

***Aquire and Implement* (AI)**	
AI2 Memperoleh dan Memelihara Perangkat Lunak	
AI2.4	Keamanan Aplikasi dan Ketersediaan
AI2.10	Pemeliharaan Perangkat Lunak Aplikasi
AI3 Memperoleh dan Mempertahankan Infrastruktur	
AI3.2	Perlindungan Sumber Data Infrastruktur dan Ketersediaan
AI3.3	Pemeliharaan Infrastruktur
***Delivery and Support* (DS)**	
DS3 Mengelola Kinerja dan Kapasitas	
DS3.4	Ketersediaan Sumber Daya
DS3.5	Pemantauan dan Pelaporan
DS 4 Memastikan Pelayanan yang Berkelanjutan	
DS4.9	Penyimpanan *backup* di luar lokasi
DS5 Memastikan Keamanan Sistem	
DS5.1	Manajemen keamanan
DS5.2	Rencana Keamanan IT
DS5.3	Manajemen Identitas
DS5.4	Pengelolaan akun pengguna
DS5.5	Pengujian keamanan, pengawasan, dan pemantauan
DS5.9	Perangkat lunak berbahaya pencegahan, deteksi, dan koreksi
DS5.10	Keamanan Jaringan
DS11 Manajemen Data	
DS11.1	Data manajemen Sistem
DS11.2	Pengaturan penyimpanan dan retensi
DS11.4	Penghapusan
DS11.5	*Backup* dan *restore* data
DS12 Mengelola Lingkungan Fisik	
DS12.1	Pemilihan lokasi dan tata letak
DS12.2	Tindakan pengamanan fisik
DS12.3	Akses fisik
DS12.4	Perlindungan terhadap faktor lingkungan
DS12.5	Pengelolaan fasilitas fisik
DS13 Mengelola Operasi	
DS13.1	Prosedur dan instruksi operasi
DS13.2	Penjadwalan Pekerjaan
DS13.3	Pemantauan infrastruktur teknologi informasi
DS13.5	Pemeliharaan preventif untuk perangkat keras

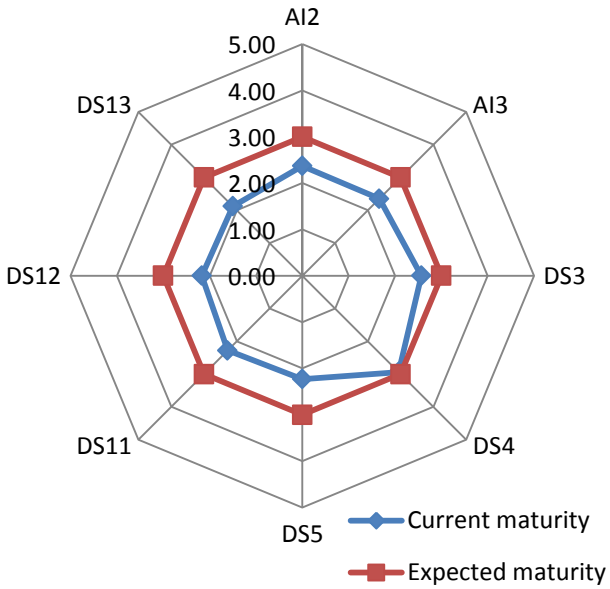
Selanjutnya setelah tahap identifikasi masalah, peneliti mendapatkan jenis kebutuhan, dan pada tahap jenis kebutuhan digolongkan menjadi 2, yaitu kebutuhan fungsional dan non fungsional. Kebutuhan fungsional yaitu kebutuhan yang terkait dengan fungsi sistem sedangkan kebutuhan non fungsional terkait dengan *tools* untuk pengembangan sistem informasi baik perangkat keras maupun perangkat lunak.

Rata-rata hasil perhitungan tata kelola teknologi informasi pada BPR XYZ dijabarkan dalam tabel berikut ini :

Tabel 4. Rekapitulasi Hasil Tingkat Kematangan

Domain	Keterangan	Nilai
AI2	Memperoleh dan Memelihara Perangkat Lunak	2,37
AI3	Memperoleh dan Mempertahankan Infrastruktur	2,35
DS3	Mengelola Kinerja dan Kapasitas	2,57
DS4	Memastikan Pelayanan yang Berkelanjutan	2,94
DS5	Memastikan Keamanan Sistem	2,23
DS11	Manajemen Data	2,28
DS12	Mengelola Lingkungan Fisik	2,17
DS13	Mengelola Operasi	2,12

Secara rata-rata tata kelola teknologi informasi pada BPR XYZ memiliki nilai 2,38, dan berada dalam skala dari 1,51 – 2,50. Artinya berada pada posisi ke 2(dilakukan tetapi belum baku / *repeatable but intuitive*). Standarisasi prosedur dan dokumentasi terkait tata kelola tekonologi informasi masih belum dibakukan, sehingga penyimpangan mungkin tidak dapat terdeteksi. Berdasarkan tingkat kematangan saat ini dan nilai tingkat kematangan yang diharapkan dapat dibuat representasinya dalam bentuk grafik radar (Gambar3).



Gambar 3. Grafik Model Kematangan

Dari grafik di atas dapat diketahui bahwa tingkat kematangan terendah berada pada proses DS13 yang mewakili proses mengelola operasi, yaitu 1,67 dan proses DS4 yang mewakili proses memastikan pelayanan yang berkelanjutan memilikit tingkat kematangan tertinggi yaitu 2,94. Adanya kebijakan perusahan penempatan penyimpanan backup data di luar lokasi memberikan kepastian pelayanan yang berkelanjutan. Hasil perhitungan tingkat kematangan menunjukkan adanya *GAP* sebesar (-0,62), *a*ntara tingkat kematangan saat ini dengan tingkat kematangan

yang diharapkan.

IV. PENUTUP

Hasil pengukuran tata kelola teknologi informasi pada BPR XYZ terdapat proses DS13 yang memiliki nilai 2,12. Nilai tersebut yang paling rendah dibanding dengan proses lainnya, sehingga membutuhkan prioritas lebih untuk ditingkatkan kematangannya sesuai level kematangan yang diharapkan. Proses DS4 memiliki tingkat kematangan tertinggi dengan nilai 2,94, hasil ini dikarenakan perusahaan memiliki peraturan harus ada penyimpanan backup data yang di luar kantor. Rata-rata proses tata kelola teknologi informasi memiliki tingkat kematangan dengan nilai 2,38 yang berada pada skala level 2 (sudah dilakukan tetapi belum baku).

DAFTAR PUSTAKA

[1] R. Huang, R. W. Zmud, and R. L. Price, "Influencing the effectiveness of IT governance practices through steering committees and communication policies," *Eur. J. Inf. Syst.*, vol. 19, no. 3, pp. 288–302, 2010.

[2] ISACA, "IT Standards , Guidelines , and Tools and Techniques for Audit and Assurance and Control Professionals," Rolling Meadows, 2010.

[3] W. Van Grembergen and S. De Haes, *Implementing Information Technology Governance : Models, Practices, and Cases*, 1st ed. New York: IGI Publishing, 2008.

[4] R. S. Debreceny and G. L. Gray, "IT Governance and Process Maturity: A Multinational Field Study," vol. 27, no. 1, pp. 157–188, 2013.

[5] D. Ramadhanty, "Penerapan Tata Kelola Teknologi Informasi Dengan Menggunakan COBIT Framework 4.1 (Studi Kasus pada PT. Indonesia Power)," Universitas Indonesia, Jakarta, 2010.

[6] ITGI, *Management Guidelines*. Rolling Meadows: IT Governance Institute, 2000.

[7] ITGI, "COBIT Framework 4.1," Rolling Meadows, 2007.

[8] S. Senft and F. Gallegos, *Information Technology Control and Audit*, 3rd ed. New York: Auerbach Publications, 2009.